HOMELAND SECURITY TERMS AND DEFINITIONS

911 (9-1-1): Used to describe the 911 telephone systems, Public Safety Answering Points and associated radio and data systems used to receive calls for assistance from the public, catalog and triage information, direct responders to emergency locations and provide support to field responders until event closure or until particular functions are assumed by others under ICS.

Adversary: Often used as a term to describe an enemy; the term enemy is reserved to indicate adversaries engaged in lethal operations against US forces.

ADNET: Anti-Drug Network. Data sharing system established in the Defense Appropriations Act of 1990 and run by the U.S. Department of Defense. Uses real-time secure communications, data sharing, and data analysis for counter drug efforts.

Anti-Terrorism: Preventive in nature and it entails using "passive and defensive measures… such as education, foreign liaison training, surveillance, and counter-surveillance, designed to deter terrorist activities." It is an "integrated, comprehensive approach … to counter the terrorist threat. The concept has two phases: proactive and reactive. The proactive phase encompasses the planning, resourcing, preventive measures, preparation, awareness education, and training that take place before a terrorist incident. The reactive phase includes the crisis management actions taken to resolve a terrorist incident." (JCS Pub 1-02)

Area Command (Unified Area Command): An organization established (1) to oversee the management of multiple incidents that are each being handled by an ICS organization or (2) to oversee the management of large or multiple incidents to which several Incident Management Teams have been assigned. Area Command has the responsibility to set overall strategy and priorities, allocate critical resources according to priorities, ensure that incidents are properly managed, and ensure that objectives are met and strategies followed. Area Command becomes Unified Area Command when incidents are multi-jurisdictional. Area Command may be established at an emergency operations center facility or at some location other than an incident command post. (NIMS)

Assessment: The evaluation and interpretation of measurements and other information to provide a basis for decision making (NIMS).

Assisting Agency: An agency or organization providing personnel, services or other resources to the agency with direct responsibility for incident management. (NIMS)

Asset: Anything that has value to the organization (ISO I3335-1:1996)

Attack: A discrete malicious action of debilitating intent inflicted by one entity upon another. A threat might attack a critical infrastructure to destroy or incapacitate it.

Awareness: The continual process of collecting, analyzing, and disseminating intelligence, information, and knowledge to allow organizations and individuals to anticipate requirements and to react effectively. (NIMS Coordinating Draft)

Biological Agents: The FBI WMD Incident Contingency Plan defines biological agents as microorganisms or toxins from living organisms that have infectious or noninfectious properties that produce lethal or serious effects in plants and animals.

Bioshield (Project): In his State of the Union Address, President Bush announced Project BioShield - a comprehensive effort to develop and make available modern, effective drugs and vaccines to protect against attack by biological and chemical weapons or other dangerous pathogens. Project BioShield will: Ensure that resources are available to pay for "next-generation" medical countermeasures. Project BioShield will allow the government to buy improved vaccines or drugs for smallpox, anthrax and botulinum toxin. Use of this authority is currently estimated to be $6B over ten years. Funds would also be available to buy countermeasures to protect against other dangerous pathogens, such as Ebola and plague, as soon as scientists verify the safety and effectiveness of these products. Strengthen NIH development capabilities by speeding research and development on medical countermeasures based on the most promising recent scientific discoveries; and gives FDA the ability to make promising treatments quickly available in emergency situations - this tightly controlled new authority can make the newest treatments widely available to patients who need it in a crisis.

Bioterrorism: The intentional use of microorganisms, or toxins, derived from living organisms, to produce death or disease in humans, animals, or plants.

Bioterrorism Response Advisory Committee (BRAC): Committee consisting of the Department of Health partners and stakeholders that advises the Department of Health on the creation of its plan for bioterrorism preparedness and response.

Block Grant: Federal grant funds that are allocated based on a predetermined statutory formula.

Catastrophic Incident: Any natural or manmade incident, including terrorism, which leaves unprecedented levels of damage and disruption severely affecting the population, infrastructure, environment, and economy. A catastrophic event would result in sustained national impacts over a prolonged period of time. (NRP Coordinating Draft)

Category "A" Diseases/Agents: The possible biological terrorism agents having the greatest potential for adverse public health impact with mass casualties. High-priority agents include organisms that pose a risk to national security because they can be easily disseminated or transmitted from person to person; result in high mortality rates and have the potential for major public health impact; might cause public panic and social disruption; and require special action for public health preparedness. The Category "A" agents are: smallpox, anthrax, plague, botulism, tularemia, and viral hemorrhagic fevers (e.g., Ebola and Lassa viruses)

Category "B" Diseases/Agents: Second highest priority agents include those that are moderately easy to disseminate; result in moderate morbidity rates and low mortality rates; and require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance. Category B diseases are: Brucellosis, epsilon toxin of *Clostridium perfringens,* food safety threats (e.g., *Salmonella* species, *Escherichia coli* O157:H7, and *Shingella)*, glanders, melioidosis, psittacosis, Q fever, ricin toxin, staphylococcal enterotoxin B, typhys fever, viral encephalitis (e.g., Venezuelan equine encephalitix, eastern and western encephalitis), and water safety threats (e.g., *Vibrio cholerae, Cryptosporidium parvum).*

Category "C" Diseases/Agents: Third highest priority agents include emerging pathogens that could be engineered for mass dissemination in the future because of the availability; ease of production and dissemination; and potential for high morbidity and mortality rates and major health impact. The CDC cites Nipah virus and hantavirus as examples.

C-DAT: Columbia Data Analysis Teams. Pilot project sponsored by the FBI and U.S. Department of Justice. C-DAT will be a complete information sharing and integration initiative, compiling data from all possible law enforcement agencies – local, state, and federal in a tri-state area (Washington, Oregon, and Idaho).

Channel of Communication: The official conduit for information flow and coordination of plans, resources, and activities.

Chemical Agents: The Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Incident Contingency Plan defines chemical agents as solids, liquids, or gases that have chemical properties that produce lethal or serious effects in plants and animals.

Choking Agents: Compounds that injure an unprotected person chiefly in the respiratory tract (the nose, throat and particularly the lungs). In extreme cases, membranes swell, lungs become filled with liquid, and death results from lack of oxygen; thus these agents "choke" an unprotected person. Choking agents include phosgene, diphosgene, and chlorine.

Civil Support: Department of Defense support to US civil authorities for domestic emergencies, and for designated law enforcement and other activities. Also called CS. (JCS Pub 1-02)

Command and Control: The exercise of authority and direction by a properly designated commander over assigned or attached forces in the accomplishment of the mission; command and control functions are performed through an arrangement of personnel, equipment, communications, computers, facilities, and procedures employed by a commander in planning, directly coordinating, and controlling forces and operations in the accomplishment of the mission (JCS Pub 1-02).

Common Operating Picture A broad view of the overall situation as reflected by situation reports, aerial photography, and other information or intelligence (NIMS).

Communications: A method or means of conveying information of any kind from one person or place to another (JCS Pub 1-02).

Communications Security: The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. (JCS Pub 1-02).

Community Policing: a "philosophy of policing, based on the concept that police officers and private citizens working together in creative ways can help solve contemporary community problems related to crime, fear of crime, social and physical disorder, and neighborhood decay." (Trojanowicz, Robert and Bonnie Bucquerox. (1990). *Community Policing: A Contemporary Perspective.* Cincinnati: Anderson Publishing Co.

Competitive Grant: One in which eligible applicants are solicited to submit concept papers. At the conclusion of the solicitation period, all received concept papers are assessed and ranked. The highest ranked applicants are then eligible for an award upon their completion of all necessary administrative requirements. Their award amount may be linked to their ranking.

Comprehensive Emergency Management Network (CEMNET): Dedicated 2-way Very High Frequency (VHF) low-band radio system. Provides direction and control capability for state and local jurisdictions for administrative use, and during an emergency or disaster. This is an emergency management net belonging to and managed by the Washington State Military Department, Emergency Management Division.

Computer Emergency Response Team: An organization chartered by an information system owner to coordinate and/or accomplish necessary actions in response to computer emergency incidents that threaten the availability or integrity of its information systems (DoDD 5160.54).

Congregate Care Center: A public or private facility that is pre-designated and managed by the American Red Cross during an emergency, where evacuated or displaced persons are housed an fed.

Consequence Management: Measures to alleviate the damage, loss, hardship or suffering caused by emergencies. It includes measures to restore essential government service, protect public health and safety, and provide emergency relief to affected governments, businesses and individuals. Per HSPD-5

crises management and consequence management are merged to a single integrated function referred to as domestic incident management.

Container Security Initiative (CSI): Designed to help protect the United States and a large portion of the global trading system from terrorists who might use container transport to hide weapons of mass destruction and related materials without disrupting legitimate flow of cargo. There are several CSI ports that are operational: Vancouver, Goteborg, Halifax, Rotterdam, Le Havre, Bremerhaven, Hamburg, Antwerp, Singapore, Yokohama, Hong Kong, Felixstowe, and Montreal. CSI requires bilateral agreements to be created with other governments to target and pre-screen high-risk containers in overseas seaports before they are shipped to the United States. Customs inspectors (pre-screeners) will also be stationed in CSI ports, to work with their overseas counterparts.

Continuity of Government (COG): Planning to ensure the continuity of essential functions in any state security emergency by providing for: succession to office and emergency delegation of authority in accordance with applicable law; safekeeping of essential resources, facilities, and records: and establishment of emergency operating capabilities.

Continuity of Operations: Efforts taken within an entity (i.e., agency, company, association, organization, business) to assure continuance of minimum essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological and/or attack-related emergencies.

Cooperating Agency: An agency supplying assistance other than direct operational or support functions or resources to the incident management effort. (NIMS)

Coordinate: To advance systematically an analysis and exchange of information among principals who have or may have a need to know certain information to carry out specific incident management responsibilities. (NIMS)

Counterintelligence: Those activities which are concerned with identifying and counteracting the threat to security posed by hostile services, organizations, or by individuals engaged in espionage, sabotage, subversion, or terrorism (JCS Pub 1-02).

Counter-terrorism: Strategic and tactical measures taken, in a collective effort to prevent acts of terrorism as defined by the U.S. Department of Justice.

Credible Threat: The FBI conducts an interagency threat assessment that indicates that the threat is credible and confirms the involvement of a WMD in the developing terrorist incident.

Crime Prevention Through Environment Design (CPTED): A method of reducing the perception of crime, the opportunity for crime, and crime itself by altering the physical environment. Employs territoriality (creates a sense of ownership), access control (increases the perceived risk of crime to potential offenders by restructuring or denying access to crime targets), and surveillance (keep potential intruders or attackers under threat of observation).

Crisis Management: Measures to resolve a hostile situation investigate and prepare a criminal case for prosecution under Federal Law. Per HSPD-5 crises management and consequence management are merged to a single integrated function referred to as domestic incident management.

Critical Agents: The biological and chemical agents likely to be used in weapons of mass destruction and other bio-terrorist attacks. Current lists may be found on the Centers for Disease Control and Prevention Web site: http://www.bt.cdc.gov/Atent/Agentlist.asp and http://www.bt.cdc.gov/Agent/AgentlistChem.asp.

Critical Information: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (JCS Pub 1-02).

Critical Infrastructure: Those systems and assets – both physical and cyber- so vital to the States, Localities and the Nation that their incapacity or destruction would have a debilitating impact on national, state and local security, economic security, and/or public health and safety. (National Strategy for Homeland Security, p.ix, USA Patriot Act, and modified to reflect state and local perspective)

Port of Vancouver- Northwest Shipping Industry

Crossband Repeater Interconnect System: Expands the crossband repeater system capability to receive transmissions at any of several frequencies and rebroadcasts audio on one or more other radio systems operating at other frequencies.

Crossband Repeater System: The simplest crossband repeater system is a two-channel crossband repeater. These devises connect two radios operating at different frequencies.

Cyber Infrastructure: Within our critical infrastructure sectors (agriculture and food, water, healthcare and public health, emergency services, government facilities, defense manufacturing capability, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping) those cyber related (continuum of computer networks) IT systems and assets; e.g. interconnected computer networks, automated control systems, information systems, servers, routers switches and fiber optic cables that allows our critical infrastructure systems to function (see critical infrastructure definition and the National Strategy to Secure Cyberspace).

Cyberspace: Describes the world of connected computers and the society that surrounds them.

Cyberterrorism: A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda.

Data: Data is unprocessed, unanalyzed raw observations and facts.

Deconfliction Center: A process designed to prevent, coordinate or preclude duplicate investigations by two separate individuals or agencies is called Case/Subject Deconfliction. Event De-confliction is designed to ensure officer safety by preventing two tactical events happening at the same time and the same location. De-confliction systems are generally computer based, some with GIS mapping capability linked to a database.

Design, Fabrication and Construction Monitoring Programs: Typically, codes and ordinances that provide for review of new construction, conditional rezoning petitions, development plans, and special exception petitions for the purpose of decreasing the opportunity for crime and increasing the perception of safety. (For example see Plaster, Sherry and Stan Carter. (1993) *Planning for Prevention: Sarasota, Florida's Approach to Crime Prevention Through Environmental Design.* Tallahassee: Florida Criminal Justice Executive Institute)

Deterrence: The prevention of action by fear of the consequences. Deterrence is a state of mind brought about by the existence of threat of unacceptable counter action. (JCS Pub 1-02). Deterrence in the homeland security threat spectrum means an enemy does not even try faced with the evidence of planning, preparation, public mobilization, and training capable of stopping their objectives.

Disease Condition Database: Washington State's electronic repository for a wide range of health data including notifiable conditions (in development).

Disaster: As used in this plan, this term is broadly defined to include disasters and emergencies that may be caused by any natural or man-made event. A large emergency event is that one beyond a community's ability to address within its own and mutual aid resources.

Disaster or Emergency Declaration: A declaration by the President which authorizes supplemental Federal assistance under the Stafford Act. The declaration is in response to a Governor's request and may cover a range of response, recovery and mitigation assistance for state and local governments, eligible private non-profit organizations, and individuals.

Disaster Medical Assistance Team(DMAT): A DMAT is a deployable national asset that can provide triage, medical or surgical stabilization, and continued monitoring and care of patients until they can be evacuated to locations where they will receive definitive medical care. Specialty DMATS can also be deployed to address mass burn injuries, pediatric care requirements, chemical injury or contamination, etc. The DMAT program is managed by the Department of Homeland Security in coordination with the Department of Health and Human Services.

Disaster Mortuary Operational Response Team (DMORT): A DMORT is a deployable national asset that can assist local authorities in providing victim identification and mortuary services, including: temporary morgue facilities; victim identification by fingerprint, forensic dental, and/or forensic pathology/anthropology methods; and processing, preparation, and disposition of remains. The DMORT program is managed by the Department of Homeland Security in coordination with the Department of Health and Human Services.

Discretionary Grant: Federal grant funds that are distributed to states, units of local government or private organizations at the discretion of the agency administering the funds. Most discretionary grants are competitive and usually have limited funds available and a large number of potential recipients.

Domain; A major grouping of activities related to the "life cycle" of a domestic incident. The four domains are prevention, preparedness, response and recovery.

Domestic Terrorism: Domestic terrorism involves groups or individuals whose terrorist activities are directed at elements of our government or population without foreign direction.

Emergency: Absent a Presidentially declared emergency, any incident(s), human-caused or natural, that requires responsive action to protect life or property. Under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, an emergency means any occasion or instance for which, in the determination of the President, Federal assistance is needed to supplement State and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States. (NIMS)

Emergency Management Assistance Compact (EMAC) A legally binding mutual aid agreement and partnership between the States that allows them to assist one another during emergencies and disasters.

Emergency Management: The process by which the state and nation prepares for emergencies and disasters, mitigates their effects, and responds to and recovers from them.

Emergency Operations Center (EOC): The physical location at which the coordination of information and resources to support domestic incident management activities normally takes place. An EOC may be a temporary facility or may be located in a more central or permanently established facility, perhaps at a higher level of organization within a jurisdiction. EOCs may be organized by major functional disciplines (e.g. fire, law enforcement, and medical services), by jurisdiction (e.g., Federal, State, regional, county, city, tribal), or some combination thereof. (NIMS)

Emergency Operations Plan (EOP): A planning document that 1) assigns responsibility to organizations and individuals for implementing specific actions at projected times and places in an emergency that exceeds the capability or routine responsibility of any one agency; 2) sets forth lines of authority and organizational relationships, and shows how all actions will be coordinated; 3) identifies personnel, equipment, facilities, supplies, and other resources available for use during response and recovery operations; and 4) identifies steps to address mitigation issues during response and recovery activities.

Emergency Responder:

Emergency Level: Emergency responders, including fire, law enforcement and emergency medical services personnel, state proprietary or private security personnel who respond to acts or threats of terrorism. They will initiate the ICS system, assess information, take necessary actions, and begin notification of appropriate personnel. They may also likely be exposed to life-threatening hazards.

Second Level: Personnel who respond to incidents of terrorism after the initial response. They may be involved in further development of the ICS system, evacuation, triage, mass care, personnel accountability, identifying and preserving evidence, agent identification, public information, decontamination, and managing site safety. These specialized resources would include Hazardous Materials Teams, emergency medical teams, SWAT Teams, Explosive Teams, and Public Health Response Teams. They may also include other special mobilized resources.

Third Level: Personnel responsible for consequence management activities to include emergency management.

Emergency Response Coordinator: Person authorized to direct implementation of an agency's emergency response plan.

Emergency Services: A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level. In addition, state and federal response plans define emergency support functions to assist in response and recovery.

Emergency Support Function: The functional approach that groups the types of assistance that a state is most likely to need (e.g. mass care, health and medical services) as well as the kinds of federal operations support necessary to sustain state response actions (e.g., transportation, communications). ESFs are expected to support one another in carrying out their respective missions.

Essential Elements of Friendly Information: Key questions likely to be asked by adversary officials and intelligence systems about specific friendly (our) intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. Also called EEFI (JCS Pub 1-02).

Evacuation: Organized, phased, and supervised withdrawal, dispersal, or removal of civilians from dangerous or potentially dangerous areas, and their reception and care in safe areas. (NIMS)

Farmgate: The value of production for all agricultural products.

Essential and Extensively Federal Asset. An Essential and Extensively Federal Asset is a team, piece of equipment, service or supply items that provides critical life saving support or incident containment capabilities, and that is so specialized that it is not available, or available in sufficient quantities, in most locations.

Event: A planned, nonemergency activity. ICS can be used as the management system for a wide range of events, e.g., parades, concerts, or sporting events.

(FAST) U.S. and Canada Free and Secure Trade: FAST is a harmonized clearance process for shipments of known compliant importers. FAST is for shipments destined to the United States (from Canada or

Mexico) using highway mode of transport. For trucks to use FAST lane processing, the Mexican manufacturer must be C-TPAT approved, the U.S. importer (of record) must be C-certified, and the commercial driver must possess a valid FAST Commercial License. The cargo release methods for FAST shipments are the National Customs Automated Prototype (NCAP) and the Pre-Arrival Processing System (PAPS).

Federal On-Scene Commander (FOSC): Means the Federal official designated upon JOC activation to ensure appropriate coordination and overall United States government response with Federal, State and local authorities.

Federal On-Scene Coordinator (FOSC or OSC): Means the federal official pre-designated by EPA or the USCG to coordinate and direct responses to oil and hazardous substances under the NCP.

Federal Radiological Emergency Response Plan: The plan that describes the Federal response to the radiological and on-site technical aspects of an emergency in the United States and identifies the lead federal agency for the event. The events include one involving the Nuclear Regulatory Commission or state licensee, the U.S. Department of Energy or the U.S. Department of Defense property, a space launch, occurrence outside the United States but affecting the United States, and one involving radium or accelerator-produced material. Transportation events are included in those involving the U.S. Nuclear Regulatory Commission, state licensee, U.S. Department of Energy, or U.S. Department of Defense.

Federal Response Plan (FRP) The plan designed to address the consequences of any disaster or emergency situation in which there is a need for Federal assistance under the authorities of the Stafford Act. Twenty-seven Federal departments and agencies including the American Red Cross are signatories to the plan.

FINCEN: Financial Crimes Enforcement Network. A US Department of Treasury program established in 1990 to implement and oversee policies related to money laundering. FINCEN provides information sharing and strategic analysis of domestic and worldwide money laundering developments, trends, and patterns.

Fire Service (FS): Individuals, who on a full-time, volunteer, or part-time basis provide life safety services including fire suppression, rescue, arson investigation, public education, and prevention.

Focus Areas: Categories of emergency preparedness activities states must address in their Cooperative Agreements for Public Health Preparedness and Response for Bioterrorism. Focus areas cover the following topics:
Focus Area A: Preparedness Planning and Readiness Assessment
Focus Area B: Surveillance and Epidemiology Capacity
Focus Area C: Laboratory Capacity – Biological Agents
Focus Area D: Laboratory Capacity – Chemical Agents
Focus Area E: Health Alert Network (HAN)/Communications and Information Technology
Focus Area F: Communicating Health Risk and Health Information Dissemination
Focus Area G: Education and Training

Force Protection: Force protection is often used in the military sense to mean a security program designed to protect our own service members, civilian employees, family members, facilities, and equipment in all locations and situations. (Joint Tactics, Techniques, and Procedures for Antiterrorism, Joint Pub 3-07.2, 17 March 1998)

Fusion Center: An organized structure to coalesce data and information for the purpose of analyzing, linking and disseminating intelligence. A model process is like to include: extract unstructured data, extract structured data and fuse structured data. Fused data are then analyzed to generate intelligence products and summaries for tactical, operational, and strategic commanders. Types of analysis typically conducted in a fusion center include; association charting, temporal charting, spatial charting, link analysis, financial analysis, content analysis and correlation analysis.

Governmental Administrative: Elected and appointed officials responsible for public administration of community health and welfare during a WMD terrorism incident.

G-Series Nerve Agents: Chemical agents of moderate to high toxicity developed in the 1930s. Examples include tabun (GA), sarin (GB), soman (GD), and GF.

Hazard: Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome. (NIMS)

Hazardous Materials Personnel (HZ): Individuals, who on a full-time, volunteer, or part-time basis identify, characterize, provide risk assessment, and mitigate/control the release of a hazardous substance or potentially hazardous substance.

Health Alerts: Urgent messages from the CDC to health officials requiring immediate action or attention. The CDC also issues health advisories containing less urgent information about a specific health incident or response that may or may not require immediate action, and health updates, which do not require action.

Homeland Defense: The protection of US territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression. Also called HLD. See also homeland security and civil support. (JCS approved definition)

Homeland Security: (1) A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. (National Strategy for Homeland Security p.2)
(2) The preparation for, prevention of, deterrence of, preemption of, defense against, and response to threats and aggressions directed towards US territory, sovereignty, domestic populations, and infrastructure; as well as crisis management, consequence management, and other domestic civil support. Also called HLS. See also homeland defense and civil support (JCS approved definition).

Hospital Emergency Incident Command System(HEICS): HEICS is the Incident Command System (ICS) framework specific to hospitals. The system was developed by the State of California and is used by many hospitals in Washington State. It specifies the chain of command and functional positions that may be required during a hospital's response to an emergency situation.

Hotwash: An after action review for events or training that discusses what went right, what went wrong and what to do differently next time.

Incapacitating Agents: An agent that produces temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days and victims usually do not require medical treatment; however, such treatment does speed recovery.

Incident: An occurrence, either human caused or by natural phenomena, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies and other occurrences requiring an emergency response. (NIMS)

Incident Action Plan (IAP): An oral or written plan containing general objectives reflecting the overall strategy for managing an incident. It may include the identification of operational resources and assignments. It may also include attachments that provide direction and important information for management of the incident during one or more operational periods. (NIMS).

Incident Commander (IC): The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site. (NIMS)

Incident Command Post (ICP): The field location at which the primary tactical-level, on-scene command functions are performed. The ICP may be co-located with the incident base or other incident facilities and is normally identified by a green rotating or flashing light. (NIMS)

Incident Command System: A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small as well as large and complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private, to organize field-level incident management operations. (NIMS)

Incident Management Team: The Incident Commander and appropriate Command and General Staff personnel assigned to an incident. (NIMS)

Incident Objectives: Statements of guidance and direction necessary for selecting appropriate strategy(s) and the tactical direction of resources. Incident objectives are based on realistic expectations of what can be accomplished when all allocated resources have been effectively deployed. Incident objectives must be achievable and measurable, yet flexible enough to allow strategic and tactical alternatives. (NIMS)

Initial Action: The actions taken by those responders first to arrive at an incident site (NIMS).

Initial Response: Resources initially committed to an incident. (NIMS)

Information: Processed fact: reporting with or without analysis. It is often prepared for publication or dissemination in some form and is intended to inform rather than warn or advise.

Information Security: The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC (JCS Pub 1-02).

Information System: The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Also, Information systems the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate and act on information (JCS Pub 6-0).

Information Warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks (CJCSI 3210.01).

Infrastructure: The framework of interdependent networks and systems comprising identifiable industries, institution (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of governments at all levels of society as a whole.

Intelligence: The product of adding value to information and data through analysis. Intelligence is created for a purpose. It is the process by which analysis is applied to information and data to inform policy-making, decision-making, including decisions regarding the allocation of resources, strategic decisions, operations and tactical decisions. Intelligence serves many purposes among which are the identification and elimination of threat sources, the investigation and resolution of threats, the identification and treatment of security risk, the elimination of threat sources, the mitigation of harm associated with risk, preemption, response, preparation and operations related to threats and risks.

Intelligence Cycle: The process by which information and data is collected, evaluated, stored, analyzed and then produced or placed in some form for dissemination to the intelligence consumer for use. The cycle consists of: consumer, collector, evaluation, analysis, production, dissemination, consumption, and consumer.

Intelligence Products: The intelligence deliverables. They are the means by which intelligence is communicated to those who will use it. Intelligence products are not limited to written digests or summaries, reports or notes, and can also include oral warnings, alerts, advisories or notices given to the consumer when justified. It also includes oral briefings and other presentations made by the intelligence professional within the scope of his or her duties and responsibilities.

Interagency Incident Management Group (IIMG): The IIMG is made up of senior representatives from Federal departments and agencies, non-governmental organizations, as well as DHS components to facilitate national-level situation awareness, policy coordination, and incident coordination.

International Terrorism: Involves groups or individuals whose terrorist activities are foreign-based and/or directed by countries or groups outside the United States whose activities transcend national boundaries.

Interoperability: The ability of systems or communications to work together.

Joint Field Office (JFO): Federal activities at a local incident site will be integrated during domestic incidents to better facilitate coordination between Federal, state, and local authorities. The JFO is expected to incorporate existing entities such as the Joint Operations Center, the Disaster Field Office and other Federal offices and teams that provide support on scene.

Joint Information Center (JIC): A facility established to coordinate all incident-related public information activities. It is the central point of contact for all news media at the scene of the incident. Public information officials from all participating agencies should collocate at the JIC. (NIMS)

Joint Information System (JIS): Integrates incident information and public affairs into a cohesive organization designed to provide consistent, coordinated, timely information during crisis or incident operations. The mission of the JIS is to provide a structure and system for developing and delivering coordinated interagency messages; developing, recommending, and executing public information plans and strategies on behalf of the IC; advising the IC concerning public affairs issues that could affect a response effort; and controlling rumors and inaccurate information that could undermine public confidence in the emergency response effort. (NIMS)

Jurisdiction: A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, state or federal boundary lines) or functional (e.g., law enforcement, public health). (NIMS).

Laboratory Levels (A,B,C,D): A system for classifying laboratories by their capabilities:
A: Routine clinical testing. Includes independent clinical labs and those at universities and community hospitals.
B: More specialized capabilities. Includes many state and local public health laboratories.
C: More sophisticated public health labs and reference labs such as those run by CDC.

D: Possessing sophisticated containment equipment and expertise to deal with the most dangerous, virulent pathogens and include only CDC and DOD labs, the FBI, and the U.S. Army Medical Research Institute of Infectious Diseases.

Lead Agency: Agency, entity, or combination of, that is recommended by the Committee on Homeland Security to the Emergency Management Council to develop a proposal for the use and application of specific grants in support of the state strategic plan on terrorism. They would also manage the grants following guidelines developed and approved by the Emergency Management Council.

Liaison: An agency official sent to another agency to facilitate interagency communications and coordination.

Law Enforcement (LE): Individuals, full-time, or on a voluntary basis, who work for agencies at the local, municipal and state levels with responsibility as sworn law enforcement officers.

Local Emergency Planning Committee (LEPC): A term used in the Emergency Planning and Community Right-to-Know Act (EPCRA) (42 U.S.C. 11001: 1986). EPCRA also known as Title II of SARA (Superfund Amendments and Reauthorization Act), was enacted by Congress as the national legislation on community safety. It was designed to help local communities protect public health, safety, and the environment from chemical hazards. To implement EPCRA Congress required each state to appoint a State Emergency Response Commission (SERC) and required each SERC to divide their state into emergency planning districts and to name a local Emergency Planning Committee (LEPC) for each district. Board representation by fire fighters, hazardous materials specialists, health officials, government and media representatives, community groups, industrial facilities, and emergency managers helps ensure that all the necessary perspectives are represented on the LEPC.

Local Government: A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional, or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. (See Section 2 (10), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002).

Logistics: Providing resources and other services to support incident management. (NIMS)

Major Disaster: As defined under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122), a major disaster is:

any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance under this Act to supplement the efforts and available resources of States, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby.

Mitigation: The activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during or after an incident. Mitigation measures are often informed by lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. It may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses and the public on measures they can take to reduce loss and injury. (NIMS).

Mobilization: The process and procedures used by all organizations federal, State, and local for activating, assembling, and transporting all resources that have been requested to respond to or support an incident. (NIMS)

MultiJurisdictional Incident: An incident requiring action from multiple agencies that each have a statutory jurisdiction to manage certain aspects of an incident. In ICS, these incidents will be managed under Unified Command.

Mutual Aid Agreement: Written agreement between agencies and/or jurisdictions in which they agree to assist one another upon request, by furnishing personnel and equipment.

National Disaster Management Medical System: A cooperative, asset-sharing partnership between the Department of Health and Human Services, the Department of Veterans Affairs, the Department of Homeland Security, and the Department of Defense. NDMS provides resources for meeting the continuity of care and mental health services requirements of the Emergency Support Function 8 in the Federal Response Plan. (NIMS)

National Homeland Security Operations Center (HSOC): The HSOC will serve as the primary national-level hub for operational communications and information pertaining to domestic incident management. Located at DHS headquarters, the HSOC will provide threat monitoring and situational awareness for domestic incident management on a 24/7 basis.

National Incident Management System (NIMS): A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and tribal governments; the private-sector, and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size or complexity. To provide for interoperability and compatibility among Federal, State, local, and tribal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multiagency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking and reporting of incident resources. (NIMS)

National Response Plan (NRP): A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan. (NIMS)

National Security Emergency: Any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States (Executive Order 12656).

Need-to-Know: The determination by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (CIA Directive 1/7. (1998). Security Controls on the Dissemination of Intelligence Information.)

Nerve Agent: Organophosphate ester derivatives of phosphoric acid. Potent inhibitors of the enzyme acetylcholinesterase (AChE), causing a disruption in normal neurologic function. Symptoms appear rapidly with death occurring as rapidly as several minutes. Nerve agents are generally divided into G-series agents and V-series agents. They include tabun (GA), sarin (GB), soman (GD), and VX.

Nongovernmental Organization: An entity with an association that is based on interests of its members, individuals, or institutions and that is not created by a government, but may work cooperatively with government. Such organizations serve a public purpose, not a private benefit. Examples of NGOs include faith-based charity organizations and the American Red Cross. (NIMS)

Non-Persistent Agent: An agent that, upon release, loses its ability to cause casualties after 10-15 minutes. It has a high evaporation rate, is lighter than air, and will disperse rapidly. A non-persistent agent

is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.

Northwest Warning, Alert & Response Network (NWWARN) Is a local and regional information sharing and coordination system pilot project by leveraging present functioning information systems or creating a system where none exists. NWWARN is a network of professionals dedicated to protecting the region's population and critical infrastructure. The purpose is to provide credible information regarding alerts, threats, and warnings to public and private infrastructure stakeholders, law enforcement and emergency services. NWWARN disseminates and collects information using a broadcast or targeted methodology to include the use of voice, e-mail, mobile text and website updates based on the priority of the message. NWWARN also includes the ability to provide citizens the ability to pass suspicious information tips to the FBI.

Nuclear Weapons: The Effects of Nuclear Weapons (DOE, 1977) defines nuclear weapons as weapons that release nuclear energy in an explosive manner as the result of nuclear chain reactions involving fission and/or fusion of atomic nuclei.

On Scene Commander: A term used to designate the FBI person who provides leadership and direction to the federal crisis management response. The FBI OSC may or may not be the regional Special Agent in Charge (SAC).

Performance Measure: A specific measurable result for each goal that indicates successful achievement.

Physical Infrastructure: Within our critical infrastructure sectors (agriculture and food, water, healthcare and public health, emergency services, government facilities, defense manufacturing capability, information and telecommunications, energy, transportation, banking and finance, chemical and hazardous materials, postal and shipping) those tangible systems and assets; e.g., basic facilities, installations, equipment and personnel needed for a functioning system (see critical infrastructure definition).

Potential Threat Element (PTE): Any group or individual in which there are allegations or information indicating a possibility of the unlawful use of force or violence, specifically the utilization of a WMD, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of a specific motivation or goal, possibly political or social in nature. This definition provides sufficient predicate for the FBI to initiate an investigation.

Pre-Arrival Processing System (PAPS): A U.S. Customs Automated Commercial System (ACS) border cargo release mechanism that utilizes barcode technology to expedite the release of commercial shipments while processing each shipment through Border Cargo Selectivity (BCS) and the Automated Targeting System (ATS).

Preparedness: The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process. Preparedness involves efforts at all levels of government and between government and the private sector an nongovernmental organizations to identify threats, determine vulnerabilities and identify required resources. Within NIMS, preparedness is operationally focused on establishing guidelines, protocols and standards for planning, training and exercises, personnel qualifications and certification, equipment certification, and publication management. (NIMS).

Prevention: Actions to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice.(NIMS).

Priority Intelligence Requirements: Those intelligence requirements for which a commander has anticipated and stated priority in the task of planning and decision making. Also called PIRs (JCS Pub 1-02).

Principal Federal Official (PFO): The Secretary may designate a PFO during a domestic incident to serve as the personal representative of DHS locally during an incident. The PFO will oversee and coordinate Federal incident activities and work with local authorities to determine requirements and provide timely Federal assistance.

Private Sector: Organizations and entities that are not part of any governmental structure. It includes for-profit and not-for-profit, and formal and informal structures, icommerce and industry, and private voluntary organizations (PVO). (NIMS)

Public Health Regions: Local health jurisdictions are organized into 9 regions. Each region will develop a plan for resource sharing and coordinated emergency response that will align to the state emergency management plan and will include hospitals, emergency medical services, law enforcement and fire protection districts.

Push Package: A delivery of medical supplies and pharmaceuticals sent from the National Pharmaceutical Stockpile to a state undergoing an emergency within 12 hours of federal approval of a request by the state's Governor

Preparedness: Building the emergency management capability to prepare for, mitigate, respond to, and recover from natural and man-made hazards and terrorist acts through planning, training, education and exercising.

Preempt: Acting to eliminate an opponent's ability to take a specific action. We stop them before they try with our efforts in surveillance, detection, intelligence gathering/sharing, cooperation, early warning and effective command and control.

Prevent: The security procedures undertaken by the public and private sector to discourage terrorist acts. This includes: a) antiterrorism which are defensive measures used to reduce the vulnerability to terrorist acts, to include limited response and containment by local military forces and is also called AT and b) counterterrorism that are offensive measures taken to prevent, deter, and respond to terrorism. (JCS Pub 1-02) Prevention involves the stopping of an enemy before they strike with effective processes, seamless interactive systems, and comprehensive threat, and vulnerability analysis.

Protect: Protection consists of five groups of activities: hardening of positions; protecting personnel; assuming mission oriented protective posture; hardening of positions (infrastructure); protecting people; using physical defense measure; and reacting to an attack. (JCS Pub 1-02) In the event of a strike we successfully defend.

Radiological Dispersal Devices (RDD): A conventional explosive device incorporating radioactive material(s) sometimes referred to as a "dirty bomb."

Rapid Response Information System (RRIS): A system of databases and links to Internet sites providing information to federal, state, and local emergency officials on federal capabilities and assistance available to respond to a consequences of a WMD/terrorism incident. This information is available to designated officials in each state, the ten FEMA regions, and key federal agencies via a protected Internet site and indirectly to the Intranet site through their respective state counterparts. It can be used as a reference guide, training aid, and an overall planning and response resource for WMD/terrorism incidents.

Reasonable Suspicion: When information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there

is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. (28 CRF 23.20 (c).

Recovery: The development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to provide housing and to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration; evaluation of the incident to identify lessons learned; post-incident reporting; and development of initiatives to mitigate the effects of future incidents (NIMS).

Resources: Personnel and major items of equipment, supplies and facilities available or potentially available for assignment to incident operations and for which status is maintained. Resources are described by kind and type and may be used in operational support or supervisory capacities at an incident or at an EOC. (NIMS)

Red Team: A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities, and to anticipate possible modes of attack.

Response: Activities that address the short-term, direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. Response also includes the execution of emergency operations plans and of mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; on-going public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice. (NIMS).

Risk Management Based Intelligence: An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source; a means of providing strategic intelligence for planning and policy making especially regarding vulnerabilities and counter-measures designed to prevent criminal acts; a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability or modality; can be quantitative if a proper data base exists to measure likelihood, impact and calculate risk; can be qualitative, subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision making in strategic planning and for operations in tactical situations. (David Schwendiman, *Risk Management Model).*

Sentinel Surveillance: Looking at the background level to check for the presence of disease. An example would be when the Department of Health contracts with a farmer to raise chickens then tests the blood of the chickens for the presence of disease.

State: When capitalized refers to any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands and any possession of the United States. See section 2 (14) of the Homeland Security Act of 2002, Pub.L. 107-296, 116 Stat.2135, (2002).

Strategic Elements: Strategic elements are those characterized by continuous long-term, high-level that involves the adoption of long-range goals and objectives, the setting of priorities; the establishment of budgets and other fiscal decisions, policy development, and the application of measures of performance or effectiveness..

Strategic Goal: Broad statement that describes what we must be able to do to successfully accomplish our mission within each strategic perspective/theme.

Strategic Mission: The tasks assigned to an individual or unit that indicates the actions to be taken. (JCS Pub 1-02) Reflects what we do – the job of homeland security.

Strategic Objective: A specific statement of how a goal will be accomplished.

Strategic Performance Measure/Benchmark: A statement of how attainment of the goal will be measure; the benchmark specifies the criterion for success. What we measure, count and report.

Strategic Planning: The systematic identification of opportunities an threats that lie in the future environment, both external and internal, which, in combination with other relevant data such as threats, vulnerabilities and risks, provides a basis to make better current decisions to pursue opportunities and to avoid threats. It is an orderly process which, sets for basic objectives and goals to be achieved, and strategies to reach those goals and objectives with supporting action plans to make sure that strategies are properly implemented.

Strategic Target: The level we want to achieve within a performance measure/benchmark.

Strategic Theme: Areas we must excel at in order to accomplish our mission.

Strategic Visions: An idealized statement of the best possible future.

Supplanting: Deliberately reducing state or local funds because of the existence of federal funds.

Surge Capacity: Ability of institutions such as clinics, hospitals or public health laboratories to sharply increased demand for their services during an emergency.

Terrorism: Terrorism includes the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (NRP Draft)

Terrorist Incident: The FBI defines a terrorist incident as a violent act, or an act dangerous to human life, in violation of the criminal laws of the United States or of any State, to intimidate or coerce a government, the civilian population or any segment thereof in furtherance of political or social objectives.

Threat: An indication of possible violence, harm or danger.

Unified Command: An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the UC, often the senior person from agencies ad/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP. (NIMS)

United States: When used in relation to section 311(a)(5) of the CWA, means the States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, Guam, American Samoa, the United States Virgin Islands, and the Pacific Island Governments.

Unity of Command: The concept by which each person within an organization reports to one and only one designated person. The purpose of unity of command is to ensure unity of effort under one responsible commander for every objective. (NIMS).

Volunteer: For purposes of the NIMS, a volunteer is any individual accepted to perform services by the lead agency, which has authority to accept volunteer services, when the individual performs services without promise, expectation, or receipt of compensation for services performed. See 16 U.S.C. 742f(c)) and 29 CFR 553.101. (NIMS)

Vulnerability: (1) The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (2) The characteristics of a system that cause it to suffer a definite degradation (incapacity to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural

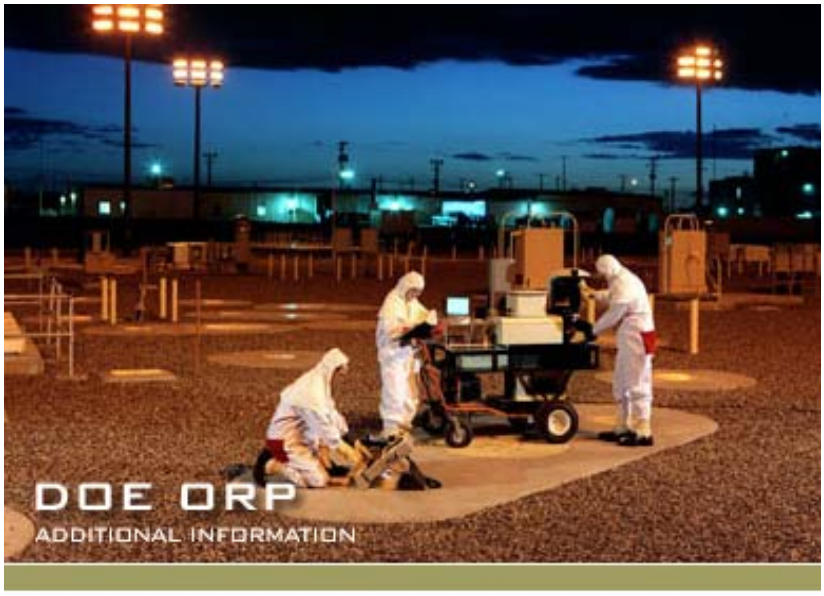
(manmade) hostile environment. (3) In information operations, a weakness in information systems security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system (JCS Pub 1-02).

Vulnerability Assessment: The Vulnerability Assessment provides a measure to indicate the relative likelihood that a particular facility or incident within the jurisdiction may become the target of a terrorist attack. The factors considered include measures of attractiveness and impact.

Watchout Situations: In fire management and fire service, watchout situations are indicators or trigger points that remind firefighters to reanalyze or to re-evaluate their suppression strategies and tactics. The "watchout situations" in the fire service are more specific and cautionary than the "Ten Standard Fire Orders." In antiterrorism, the term is used as a metaphor for those observations that can alert trained personnel not just firefighters but law enforcement, public works, private security, or anyone, to be more cautious, more observant, and more likely to report the unusual behavior or activity to the appropriate authorities.

Weapons of Mass Destruction: As defined in Title 18, USC 2332a: (A) Any explosive, incendiary or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, or a missile having an explosive or incendiary charge of more than one quarter ounce, or mine or device similar to the above; (B) Any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;(C) Any weapon involving disease organism, or (D) Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (NRP Coordinating Draft)

Zoonotic: Of or relating to zoonosis. An animal disease that can be transmitted to humans, (e.g. ebola, lyme disease, anthrax, rabbit fever, rabies, and swamp fever).



US DOE Hanford Nuclear Reservation, WA